

Titel	Professionelle Angriffsprävention durch ReCoB-Systeme	Schlüsselworte	ReCoBS, Remote Controlled Browser System, TightGate™-Pro
Autor	Patrick Leibbrand / p.leibbrand@m-privacy.de	Datum	21.12.11
Redaktion	Patrick Leibbrand / p.leibbrand@m-privacy.de	Version	1.5

0 Ausgangssituation

Täglich werden Arbeitsplatzrechner in Unternehmen aller Art weltweit Ziel von Angriffen aus dem Internet - trotz Schutzmaßnahmen wie Firewalls, Virenschernern und Intrusion Detection Systems. Mit teils enormem administrativem Aufwand versucht man gerade in Bereichen mit erhöhtem Sicherheitsbedarf, ein notwendiges Schutzniveau aufrecht zu erhalten. Dennoch attackieren Angreifer aus dem Internet gezielt Arbeitsplatzrechner im internen Netzwerk von Firmen und Behörden, oft unter Ausnutzung von Sicherheitslücken der darauf installierten Programme. Industriespionage, unberechtigter Abfluss sensibler Interna zu unbefugten Dritten und massive Beeinträchtigung des Systembetriebs durch Manipulation von Daten und Programmen sind die unmittelbaren Folgen.

1 Gefahr durch Internetzugriff

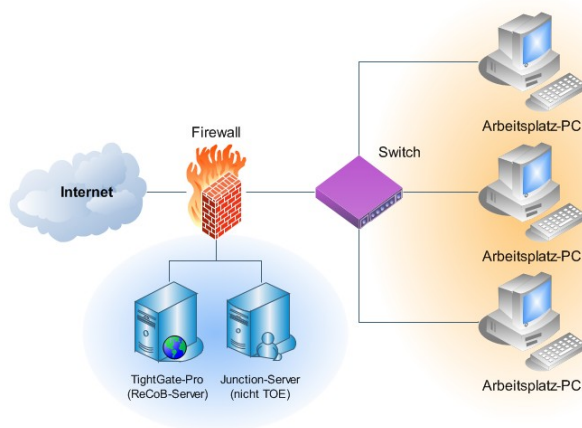
Moderne Computerarbeitsplätze erfordern häufig Internetzugriff. Viele Informationen sind in der gebotenen Aktualität und Detailliertheit nur online verfügbar, zudem werden Geschäftsstellen und Unternehmensbereiche immer stärker vernetzt. Die auf Arbeitsplatzrechnern installierten Anwenderprogramme greifen in vielen Fällen funktionsbedingt unbehelligt von konventionellen Schutzmaßnahmen auf das Internet zu. Dies betrifft vor allem Webbrowser, jedoch auch E-Mail-Programme, PDF-Viewer oder Multimediaapplikationen. Sicherheitslücken werden mit zunehmender Funktionenvielfalt und Komplexität der Anwendungen wahrscheinlicher. Jede Schwachstelle birgt das Potenzial eines Angriffs auf den betreffenden Rechner und das interne Netzwerk mit u. U. weitreichenden Konsequenzen. Zugleich erlaubt es die Architektur gängiger Betriebssysteme nur eingeschränkt, Auswirkungen von Sicherheitslücken installierter Programme zu neutralisieren, etwa durch ein hinreichend engmaschiges Berechtigungskonzept. Daraus folgt, dass sich interne Rechner und Netzwerke mittels konventioneller Verfahren nicht effektiv gegen Angriffe aus dem Internet schützen lassen.

Kommt ein Verzicht auf den Internetzugriff aus organisatorischen Gründen nicht infrage, wird bisweilen auf vollständig separate Netzwerke zurückgegriffen. Letztere erfordern jedoch organisatorisch und materiell einen unverhältnismäßig hohen Aufwand.

2 Angriffsprävention durch ReCoBS

Starken Schutz gegen Angriffe aus dem Internet über Sicherheitslücken in Anwenderprogrammen bieten sogenannte Remote-Controlled Browser Systems (ReCoBS). Auch hier handelt es sich de facto um eine physikalischen Trennung der Netzwerke, jedoch mit wesentlich weniger Aufwand und Kosten bei zugleich weitaus besserer Bedienbarkeit im Vergleich zu bisherigen Ansätzen. Ein ReCoBS isoliert potenziell gefährdete Applikationen vom Arbeitsplatzrechner bzw. dessen Netzwerk und verhindert damit Übergriffe aus dem Internet auf interne Daten und Systeme. Internetbrowser, E-Mail-Programm und weitere Anwendungen wie beispielsweise der Adobe Reader werden dabei auf einem getrennten, dem Unternehmensnetzwerk vorgelagerten Schutzsystem ausgeführt. Lediglich die Bildschirmausgabe wird über ein funktionspezifisches Protokoll an die Arbeitsplatzstation durchgereicht und Maus- sowie Tastatursignale in umgekehrter Richtung an das ReCoBS übermittelt. Internetgebundene Applikationen wie vor allem der Webbrowser können ohne Gefährdung interner Infrastrukturen genutzt werden. Neben dem Schutz vor einer Manipulation der Rechner und Netzwerkkomponenten wird auch unberechtigtem Datenabfluss in das Internet zuverlässig vorgebeugt. Moderne ReCoB-Systeme sind un-

kompliziert in professionelle Unternehmensinfrastrukturen integrierbar und entfalten ihre Schutzfunktion nach initialer Konfiguration transparent und technisch unabhängig von anderweitigen Maßnahmen.



Die Grafik illustriert den prinzipiellen Aufbau des Gesamtsystems. Die Arbeitsplatzrechner werden über einen Paketfilter, der nur die notwendigen Pakete des ReCoBS passieren lässt, mit der Bildschirmausgabe der Applikationen versorgt, die wiederum auf dem vorgelagerten Server ausgeführt werden. Das ReCoB-System wird vorzugsweise hinter der ersten Firewall des Firmennetzwerks in der Demilitarisierten Zone (DMZ) installiert. Der Junction-Server stellt zusätzliche Dienste fakultativ zur Verfügung und ist kein zwingend notwendiger Systembestandteil.

3 Marktführend: das ReCoB-System TightGate™-Pro

Leistungsfähige ReCoB-Systeme, die den strengen Kriterien des ReCoBS-Schutzprofils des BSI (PP-0040) entsprechen, entwickelt die Berliner m-privacy GmbH mit den Serverprodukten der TightGate™-Produktlinie. TightGate™-Pro ermöglicht die Versorgung von Rechnerarbeitsplätzen mit vollfunktionalem Internetzugang ohne Risiko eines An- oder Übergriffs auf das interne Netzwerk.

TightGate™-Pro der m-privacy GmbH wird deutschlandweit von Unternehmen sowie Bundes- und Landesbehörden zum Schutz ihrer Netzwerke verwendet, u. a.

- Presse- und Informationsamt der Bundesregierung
- Polizei- und Justizbehörden
- Dienststellen von Landesdatenschutzbeauftragten
- Weitere Organisationen aus Industrie und öffentlicher Verwaltung

Eine Zertifizierung von TightGate™-Pro (CC) Ver. 1.4 nach Common Criteria beim Bundesamt für Sicherheit in der Informationstechnik (BSI-DSZ-CC-0589) wird derzeit angestrebt.

Vorteile einer ReCoBS-Lösung mit TightGate™-Pro:

- Zuverlässiger Schutz interner Infrastrukturen vor Angriffen aus dem Internet
- Verhinderung von Datenabfluss und Betriebsspionage
- Gefahrlose Internetnutzung, auch aktiver Inhalte
- Präventives Schutzkonzept statt reaktiver Filterung
- Geringer Wartungsaufwand, zentrale Verwaltung
- Hohe Benutzerfreundlichkeit
- Geringer Schulungsaufwand, hohe Nutzerakzeptanz

4 Weiterführende Informationen

- **Informationen zu TightGate™-Pro** - www.m-privacy.de/produkte/tightgate-pro
- **Kurzinformation ReCoBS** des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) https://www.bsi.bund.de/cln_165/ContentBSI/Themen/Internet_Sicherheit/Gefahrenungen/Aktiv_inhalte/schutzmoeglichkeiten/recobs/kurzinformation.html;jsessionid=AB029DB9A050657CE902998585DB94FF